



# ACOP Reliability and Safety

Presenter: Paul Nemeth

Credits: DL



# RELIABILITY

---

- ACOP Reliability effort focuses on assuring mission success and eliminating any potential single failure points that can affect safety.
- Reliability assessment served as a foundation for subsequent Safety Analysis



# FMECA and SPF List (1)

---

- Failure Modes, Effects and Criticality Analysis is performed to:
  - ✓ Identify possible failure modes and their effects
  - ✓ Determine severity of each failure effect
  - ✓ Identify and possibly remove or control SPF  
(identified SPF are listed with rationale to accept them)



# FMECA and SPF List (2)

---

- FMECA guidelines:
  - ✓ FMECA is performed following GPQ-010-PSA-102 (Reliability and Maintainability for ESA Microgravity Facilities)
  - ✓ Reliability Categories defined according to GPQ-010-PSA-102 and NASA NSTS 1700.7B for safety categories



# FMECA - Reliability Categories

---

<b>Cat.1a: Catastrophic</b> (safety categories NSTS 1700.7B ISS Addendum)	Hazard which can result in the potential for: <ul style="list-style-type: none"><li>• a disabling or fatal personnel injury</li><li>• loss of the Orbiter/ISS, ground facilities or STS/ISS equipment</li></ul>
<b>Cat.1b: Critical</b> (safety categories NSTS 1700.7B ISS Addendum)	Hazard which can result in: <ul style="list-style-type: none"><li>• damage to STS/ISS</li><li>• a non-disabling personnel injury</li><li>• the use of unscheduled safing procedures that affect operations of the Orbiter/ISS or another payload</li></ul>
<b>Cat. 2: Major</b> (GPQ-010-PSA-102)	The failure propagates across the interface and/or the facility cannot operate anymore.
<b>Cat. 3: Significant</b> (GPQ-010-PSA-102)	The facility is partly operable (minor impact on the mission) or needs corrective on-orbit maintenance.



# FMECA - Functional Blocks

---

ACOP System identified functional blocks:

- ACOP-SBC
- ACOP-T101
- ACOP-T102
- ACOP-T103
- Mechanical Parts
- ACOP-PS
- ACOP-BP
- HARD DRIVE
- Front Panel



# FMECA - Results (1)

---

- Most identified failure modes are Severity Category 3 (On-orbit Maintainable Items)
  - minor impact on the mission

- Failures with Severity Category 1a/1b (3 cases identified):

<i><b>Item / Block</b></i>	<i><b>Assumed Failure Mode</b></i>
✓ ACOP hard drive	High rotational speed
✓ LCD (TBC)	Rupture
✓ Mechanical parts	Rupture

→ Safety Hazard Analysis has been performed according to NSTS1700.7B (Standardized Hazard Report STD-ACP-HR-001 and Unique Hazard Report ACP-HR-002)



# FMECA - Results (2)

---

- Failures with Severity Category 2 (5 cases identified) are Single Point Failures:

<i><b>Item / Block</b></i>	<i><b>Assumed Failure Mode</b></i>
✓ ACOP Backplane	Loss of function
Front panel:	
✓ HRDL Connector	Loss of function
✓ Power Connector	Loss of function
✓ MRDL Connector	Loss of function
✓ Circuit Breaker (switch)	Loss of function
→ Deeper level analysis will be performed when the detailed design will be available	





# SAFETY

---

- Safety Analyses strive to minimize the potential for the ACOP to affect/damage the AMS-02, ISS, Crew and other payloads.
- Established that the ACOP operations can not directly influence the safety of the AMS-02 in a new unique manner.



# Safety – ACOP FSDP

---

- ACOP Flight Safety Data Package for Phase 0/I Safety Review according to:
  - ✓ Programmatic Requirements of NSTS 13830, Rev. C
  - ✓ Technical Requirements of NSTS 1700.7B, ISS Addendum and NSTS 18798B



# Safety - Analysis

---

- Safety subsystems:
  - Structures
  - Electrical
  - Materials
  - Human factors
- Hazard categories:
  - Rupture / Collision
  - Injury / Illness
  - Electrical shock
  - Off-gassing / Toxicity
  - Fire
  - Temperature extremes
  - Radiation



# Safety - Hazard Reports

---

- a) ACOP Flight Payload Standardized Hazard Report STD-ACP-HR-001 (JSC Form 1230)
  
- b) ACOP Unique Hazard Reports (JSC Form 542B):
  - ✓ ACP-HR-002      Structure Failure
  - ✓ ACP-HR-003      IVA Electrical Shock



# Standardized Hazard Report (1)

---

**Following standard hazards with relevant controls are identified:**

- Sharp Edges: design according to NSTS 07700 Vol. XIV App. 9 (IVA hardware) / SSP 57000
- Shatterable Materials: LCD (TBC) protection plastic covering (LEXAN)
- Flammable Materials: A-rated selected from MAPTIS
- Material Off-gassing: Materials selected from MAPTIS with acceptable off-gassing characteristics
- Non Ionizing Radiation Non-Transmitters: SSP 30238 EMI compatibility testing



# Standardized Hazard Report (2)

---

- Touch Temperature: design according to requirements of NSTS 18798B Letter MA2-95-048 (limits of  $-18^{\circ}\text{C}$  to  $+49^{\circ}\text{C}$ )
- Electrical Power Distribution: design according to protection requirements of NSTS 18798B Letter TA-92-038
- Rotating Equipment: Hard drives are contained within hard disk case and within the metallic box of ACOP. Rotating Energy: TBD
- Mating / De-mating of Power Connectors: design according to low power criteria of NSTS 18798B letter MA2-99-170



# ACP-HR-002 Structure Failure (1)

---

- Materials selected from MSFC-HDBK-527 / JSC-09604 / MAPTIS database to meet requirements of MFSC-SPEC-522B for stress corrosion
- Fracture control plan procedures in accordance with NASA-STD-5003
- Structure (metallic) is verified by analysis using factors of 1.25 for yield and 2.0 for ultimate conditions



# ACP-HR-002 Structure Failure (2)

---

**Critical issue:** The Margin of Safety of the EXPRESS Rack attachment receptacles is negative (-0.183).

→ Possible actions to meet required positive Margin of Safety:

Possible Solutions:

1. Change the Attachment Receptacle type (increase the allowable forces)
2. Reduce the mass of ACOP
3. Move the CoG of ACOP towards the backplate to reduce the forces on the Attachment Receptacles due to bending





# ACP-HR-003 Electrical Shock

---

**High voltage source (> 32V):** DC/AC inverter installed inside ACOP to provide power for backlight of LCD display (TBC)

## **Hazard Controls:**

- ✓ ACOP must be switched-off when the front panel is opened (no power to the DC/AC inverter)
- ✓ The inverter is not accessible even when the front panel is open, since it is inside a metallic box
- ✓ Bonding and grounding as per SSP-52000-IDD-ERP and Interpretation Letter MA2-99-14



# Other Safety Issues

---

- **Fire Protection:**
  - ✓ Approved materials, proper wire sizing and circuit protection, proper grounding, conformal coating and electronic parts de-rating
  - ✓ Dedicated fire detection PFE port are not required: ACOP becomes an extension of the EXPRESS Rack Fire Event Location, interfaced with the rack AAA and smoke sensor and utilizing the rack suppression path
- **Rapid Safing:**
  - ✓ ACOP does not impede emergency IVA: hardware within an EXPRESS Rack volume
- **Operations / Maintenance:**
  - ✓ Design provision meets the requirements of Letter MA2-00-038